Retsudvalget 2014-15
REU Alm.del Bilag 60
Offentligt

Krav til kryptering

- Krypteringens krav til lovgiverne

Gert Læssøe Mikkelsen,
gert.l.mikkelsen@alexandra.dk
Alexandra Instituttet A/S

Kryptering

- Sikring af data – kommunikation
- Sikring af data – opbevaring
- Digitale signaturer – både ”maskine til maskine” og NemID

- *Smart kryptografi:*
  - *Sikring af data under brug og beregning*
  - *Kryptografisk sikring mod identitetsmisbrug*

- *Kryptering af data i Cloudløsninger*
  - *Hvad hvis nøgledata håndteres i DK?*

EU's persondataforordning - brud på persondatasikkerhed

- *"…under hensyntagen til navnlig karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede."* (68)
- "*…bør der tages hensyn til omstændighederne ved sikkerhedsbruddet, herunder til om personoplysningerne var beskyttet ved passende tekniske beskyttelsesforanstaltninger…"* (69)
- kryptering slækker kravene til dataansvarlig -> incitament til brug af kryptering

ALEXANDRA INSTITUTTET

Multiparty computation MPC - sikre flerpartsberegninger

- Beregninger på krypterede data
- Konkurrenceoptimering
- Sikre sundhedsdata (forsikringsudbetalinger)
- Case: vælgererklæringer
  - Personfølsom data (*borgeren må kun støtte ét parti*)
  - Partiet og Indenrigsministeriet
  - Brugernes data er beskyttet så længe parterne ikke samarbejder – eller begge er hacket på samme tid.

ALEXANDRA INSTITUTTET

Privacy-ABC teknologi
- sikker identitetshåndtering.

- Microsoft U-Prove
- IBM Identity Mixer

U-Prove

Identity Mixer
Security Group
IBM Research Zurich

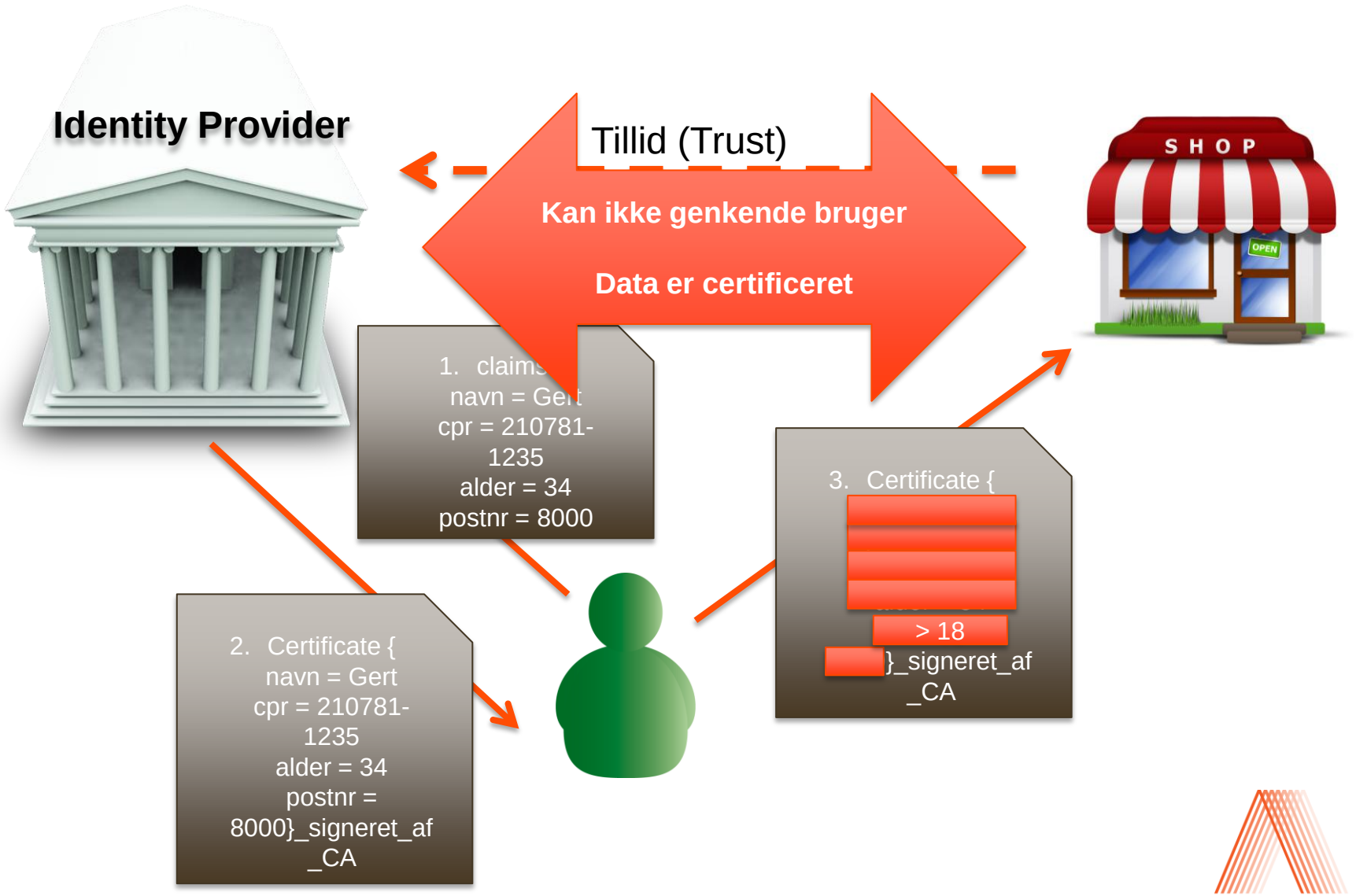
ALEXANDRA INSTITUTTET

Den fysiske verden
- en historie fra Sverige

Jeg er over 20
(Offline)

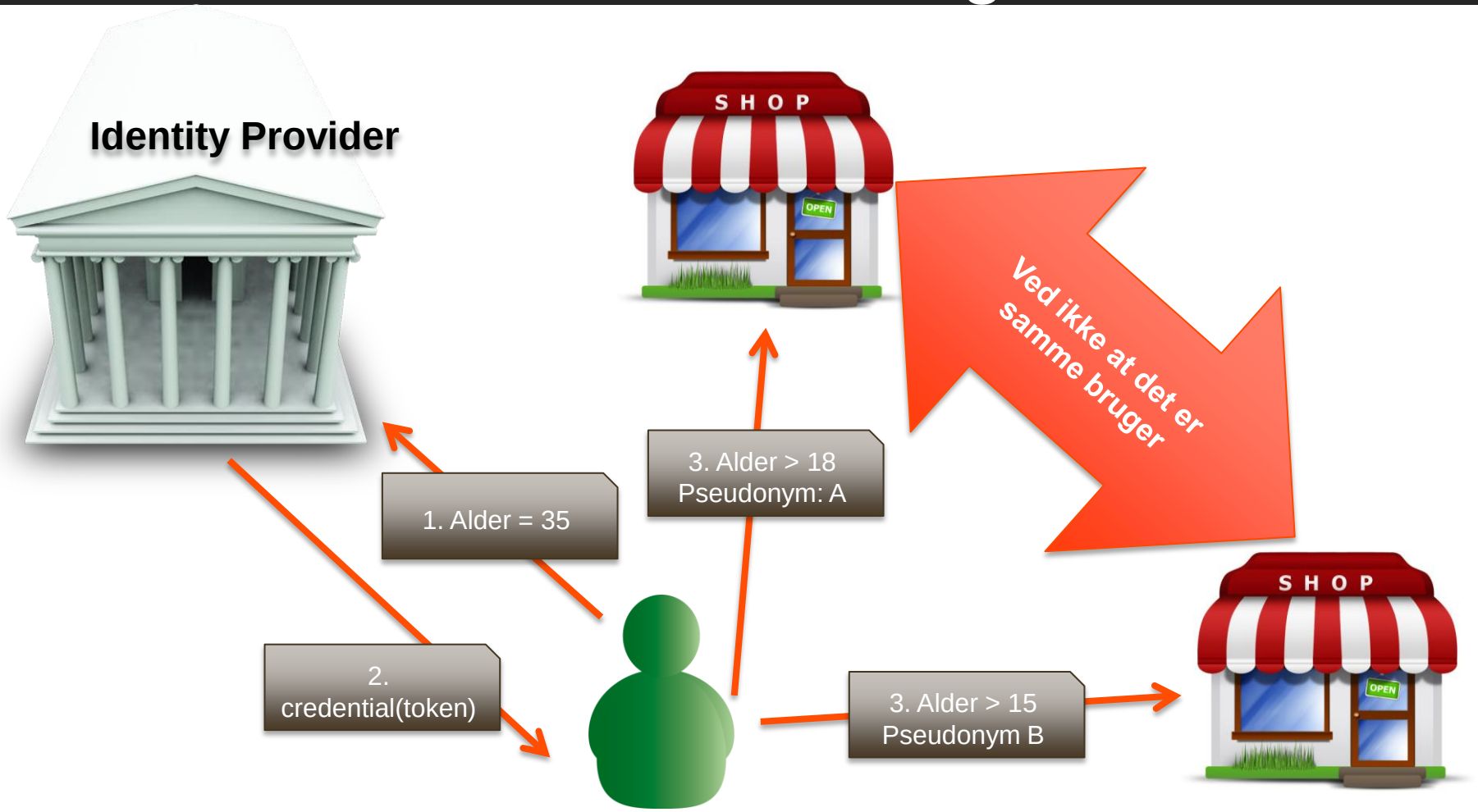
ALEXANDRA
INSTITUTTET

Privacy-ABC teknologi
- sikker identitetshåndtering.



ALEXANDRA INSTITUTTET

Privacy-ABC teknologi
- sikker identitetshåndtering.



ALEXANDRA INSTITUTTET

Teknologien kunne anvendes

- Registret Over Frivilligt Udelukkede Spillere (Rofus)
- "Hooligansregisteret" – (Lov om sikkerhed ved bestemte idrætsbegiven-heder)

ALEXANDRA INSTITUTTET

Konklusion

- Der findes kryptografisk teknologi til at højne sikkerheden omkring persondata.
- Der skal være et forretningsmæssigt incitament til at bruge *smart kryptografi*
  - *kan bla. komme fra lovgivningen.*
- Teknologi skal kunne lette juridiske aftaler.
- Forholde sig til nutiden ang. Cloud og kryptering

Tak for jeres opmærksomhed